

Testimony of Chris Kelly
Chief Privacy Officer, Facebook
Before the Oversight and Investigations Subcommittee,
House Energy and Commerce Committee
June 28, 2006

Thank you Chairman Whitfield and members of the Subcommittee for this opportunity to be with you and explain how Facebook uses technology and policy to protect people on our network.

My name is Chris Kelly, and I serve as Chief Privacy Officer of Facebook, a social utility that allows people to share information with their real world communities. I am very happy to be here today to explain how the two core ideas of social interaction and privacy guide everything that we do, and help protect people on our network. As we say in our basic statement of principles on the site, people want to share information with their friends and those around them, but they don't necessarily want to share personal information with the entire world.

I joined Facebook last September as the first Chief Privacy Officer in the social networking space, and am creating the role at an Internet company for the fourth time. In my previous service as a Chief Privacy Officer and technology attorney I have represented many clients in the technology and media industries on privacy, security, safety, and intellectual property issues. I was also part of the founding team and served as a Fellow at Harvard Law School's Berkman Center for Internet and Society, a leading think tank focused on public policy issues of the digital age.

In February of 2004, our CEO and Founder Mark Zuckerberg launched the first version of Facebook from his college dorm room. Now, Facebook is the seventh busiest site overall and runs the busiest photo site in the United States, according to independent service ComScore Networks. We have more than 8 million registered members for whom Facebook has become a core part of how they interact within their communities. Starting with our college communities, we have since expanded to offer school-focused interactions for high-school students, and more recently have followed our graduating students into the work world.

Privacy, security, and safety have been at the forefront of our concerns since the founding of the site. There is one overarching way that Facebook differs from nearly all other social networking sites – profile information is not generally available to the outside world. It is only available to Facebook members inside their individual, validated networks or through confirmed friends. We want to give people extensive power over their ability to share information, and the ability to limit who has access to it.

Of course, no protection mechanism is perfect. But the mere fact that Facebook does not make information available by default to anyone with access to the Internet, combined with the other prudent measures we have taken to focus information sharing on real-

world communities, has made a radical difference in the privacy, security, and safety of the Facebook experience.

Following this major differentiator from most sites, we have set up four levels of protection for our members that I would like to outline for you today.

First, we require validation in order to get on the site in the first place. For college students, and those high schools where it is possible, membership in the school community is proven through a valid email associated with that college or school. Where high schools do not offer students email addresses, we have instituted an invitation-based system that is designed to limit even initial access to that school network.

Second, we segment information access within networks based on real-world communities. Being a member of Facebook does not give you access to the profiles of all people on Facebook. You are only allowed to access the profiles of other members at your college, high school, work, or (with explicit user choice) geographic network, and have power to add confirmed friends in other networks. This has two positive effects. First, users are gaining more information about those around them in the real world, which has pro-social effects on campuses around the country. Second, there is a built-in neighborhood watch program, especially with respect to high schools, where abuse of the system can be easily identified and addressed.

Third, we put power in our users' hands to make choices about how they reveal information. I have mentioned already the ability to confirm friends from other networks, and the "My Privacy" tab on every navigation bar throughout the site allows users to make detailed choices about who can see particular pieces of information about them, including their contact information and photos.

Finally, we have a safety net of protection through both technological tools we deploy to detect misuse of the site and human capital dedicated to potential problems -- our 20 person and growing customer service staff, headed by a seasoned veteran and backed up by myself and two other attorneys. Most of our customer service representatives are recent graduates of outstanding colleges, and dedicated Facebook users, so they know the system inside and out. On those rare occasions where someone has attempted to misuse our network, we engage rapidly with the relevant authorities. Because the system is built for accountability with its email validation requirement and segmentation of communities, misuse is both deterred and generally detected quickly. We quickly launch an internal investigation and step in where we receive reports of the misuse of Facebook in any way.

Overall, the fact that information posted on Facebook is not generally available has made Facebook a different experience for our users, and one they clearly enjoy as reflected in their frequent visits. Our intuition about the importance of tying access to information based on the networks where people already exist in real life has been shown to have huge effect in both deterring and exposing misuse. By focusing on real-world networks as the touchstone for access, we provide both a built-in reflection of people's

expectations about who will know information about them, and restrictions that make access difficult for those who might have harmful intentions.

Facebook is proud to have led the way in giving people control over sharing information online. Thank you again for the opportunity to comment before the committee, and I look forward to your questions.